ippolita

Workshop di comunicazione e sicurezza per i centri antiviolenza

Report finale

del gruppo di ricerca Ippolita per la descrizione dell'attività formativa

Preparato per: Rete DiRe - Donne in Rete contro la violenza

10 Ottobre 2017

ippolita

Informazioni generali

Date e orari

6 – 7 ottobre 2017

Venerdi: ore 11.00 – 18.00

Sabato: ore 10.00 – 17.00

TOTALE 12 ORE

Luogo di svolgimento

Urban Center – Piazza del Nettuno, 2

Bologna

Formatrici per il Gruppo Ippolita

Lavinia Hanay Raja. Giornalista, autore e docente di Culture digitali e archeologia dei nuovi media presso NABA Nuova accademia di belle Arti di Milano.

Emanuela Cameli. Tecnica informatica e formatrice, social media editor e community manager di social network.

ippolita

Programma

Venerdì

11.00 - 11.15 Accoglienza, registrazioni e saluti

11.15 - 12.00 Brain storming in gruppo

12.00 - 13.30 Teorie della Rete. Introduzione tecno-politica: profiling, trasparenza radicale, ed esclusione sociale.

13.30 - 14.30 Pausa pranzo

14.30 – 15.00 Nuove forme di violenza contro le donne nei mondi digitale: dal cyberstalking al revenge porn.

15.00 – 16.30 Gestione di un profilo Facebook orientato al miglioramento della privacy

16.30 – 16.45 Pausa caffè

16.45 – 18.00 Come creare e sfruttare al meglio una password sicura

Sabato

10.00 – 11.30 Gamificazione e dipendenza in ambiente digitale: dalla comfort zone all'abbassamento delle difese emotive

11.30 – 13.00 Il black market degli abuser: panoramica generale sugli strumenti di sorveglianza

13.00 – 14.00 Pausa pranzo

14.00 – 16.00 Orientarsi nell'universo Android per acquisire strumenti di autodifesa digitale

16.00 – 16.15 Pausa caffè

16.15 – 17.00 Simulazione di casi in gruppi

Inquadramento teorico del corso

I servizi del web 2.0 sono l'esemplificazione del nuovo capitalismo digitale. Sono completamente gratuiti eppure costano moltissimo. Il loro profitto si basa sul profiling, l'insieme delle tecniche che permettono di classificare singoli e gruppi di utenti in base al loro comportamento. Per ottenere un migliore profiling, dunque un migliore profitto, è necessario che gli utenti riversino ogni giorno quanti più dati possibili sui server delle aziende che producono i servizi. L'architettura delle piattaforme e delle app gratuite è stata progettata in modo da stimolare il massimo grado di contenuti connessi all'identità, questo processo viene chiamato trasparenza radicale. Per agevolare l'estrazione dati gli utenti sono portati a credere che esista una confort zone da popolare attraverso la creazione di relazioni omofile. Questa falsa tranquillità viene facilmente a cadere quando i contesti collassano e non sappiamo più come dividere gli ambiti che i dispositivi ci hanno portato ad unire. Si creano dunque nuove fragilità dovute all'esposizione del sé e la cui responsabilità è da imputarsi non solo agli utenti, ma soprattutto ai servizi. Il fenomeno detto degli “haters” va inquadrato dunque anche attraverso l'analisi dell'architettura web, infatti la completa rimozione della dialettica della negatività operata dalle piattaforme agevola l'emergere di questo fenomeno. La rimozione della negatività diseduca al dissenso e mette gli utenti nella condizione di non sapere come difendersi dagli attacchi.

La quantificazione numerica di ogni intervento (post, condivisione, commento, etc) è la chiave di volta per comprendere come il servizio sia in grado di manipolare la costruzione dell'identità di ciascuno utente. Siamo immersi in un ambiente altamente performativo in cui la mancanza di valutazione (like, stelline etc) equivale a una valutazione negativa. Questo contesto stimola comportamenti collusivi e strumentali, infine de-solidarizza i rapporti tra le persone.

Oltre all'ossessione per l'incremento del proprio capitale reputazionale abbiamo un ambiente completamente gamificato (da gamification – ludicizzazione). La gamificazione mutua le proprie tecniche dal game design per trasportarle in ambienti non di gioco. Il suo obiettivo è quello di cambiare i comportamenti degli utenti attraverso la prassi del “punteggio e ricompensa”stimolando in continuazione i percorsi dopaminici. Il carico cognitivo richiesto da un ambiente gamificato è estremamente esiguo, poiché richiede più che altro l'impiego della memoria procedurale. Questa è una delle ragioni per cui non esistono i nativi digitali, infatti sia persone con difficoltà cognitive che persone al si sopra dei sessant'anni sono perfettamente in grado di interagire in questi ambienti.

Gli ambienti digitali che viviamo ogni giorno sono degli ambienti commerciali creati per abbassare le nostre difese e la nostra attenzione portandoci in uno stato di flusso dominato da automatismi indotti dal contesto. Per le donne che vivono stati di fragilità tutto questo può diventare estremamente pericoloso e va indagato nel merito delle nuove vulnerabilità sia tecniche che psicologiche che sta creando.

Si sviluppano, infatti, nuove forme persecutorie perpetrate online attraverso la diffusione di contenuti privati o con il monitoraggio delle proprie comunicazioni e degli spostamenti.

Il corso ha voluto far luce sulle tecnologie del dominio e parallelamente sulle nuove forme di violenza in rete, fornendo le conoscenze e gli strumenti tecnici utili a incrementare la sicurezza e la privacy dei profili digitali delle donne e dei propri dispositivi informatici.

MATERIALI, ATTREZZATURE E METODOLOGIE UTILIZZATE

Pc portatili, video-proiettore, slide, riferimenti bibliografici, sitografia.

Lezione frontale, esercitazioni pratiche, brain storming e simulazione di casi.

OBIETTIVI RAGGIUNTI

* Circolazione dei saperi e delle esperienze tra operatrici e volontarie dei Centri Antiviolenza;

* Conoscenza degli aspetti manipolatori che i social network operano sull'identità personale per ottenere dalle utenti quante più informazioni possibile;

* Conoscenza delle nuove forme di violenza online: quali tipologie e come agiscono;

* Conoscenza dell'aspetto "gamificato" (ludicizzato) delle architetture dei media sociali e come contribuiscano all'abbassamento delle difese emotive delle utenti, a cui segue la creazione di nuove fragilità;

* Saper fornire, in fase di prima accoglienza, assistenza tecnica di base sui profili Facebook delle donne che si rivolgono al centro e sui loro smartphone;

* Capacità di utilizzare in un caso reale le conoscenze acquisite.

Valutazione finale

Le partecipanti al corso hanno mostrato una forte motivazione nei confronti degli argomenti trattati esprimendo immediato interesse sia relativamente ai contenuti delle parti teoriche, sia alle fasi esercitativo-pratiche.

Complessivamente si è manifestato il desiderio di approfondire alcuni tra i temi che sono stati presi in esame.

Da un lato la gamification e le dipendenze digitali hanno fatto emergere le difficoltà di operatrici e volontarie nel gestire il distacco dei dispositivi mobili da parte delle donne vittime di cyberstalking, in particolar modo nei casi di donne che vivono nelle case rifugio. Lo smartphone, vissuto come mezzo fondamentale di esposizione del sé e contatto con le proprie relazioni sociali, diventa infatti protesi del proprio corpo innescando forme di dipendenza.

Dall'altro lato è emerso il desiderio di modellizzare l'esperienza finalizzandola alla creazione di uno standard minimo di sicurezza digitale utile a tutta la rete Di.Re, che possa comprendere sia la sicurezza digitale dei sistemi informatici dei Centri Antiviolenza, sia la stesura di linee guida dedicate alla diagnostica delle problematiche dei profili digitali (e dei dispositivi) delle donne vittime di violenza.

La parte esperienziale, di esercitazione e simulazione, ha aiutato a fissare i concetti chiave e a immergere le partecipanti in una situazione tipica di un Centro Antiviolenza.

I casi di analisi proposti hanno permesso, infatti, di applicare le tecniche e i metodi appresi durante la formazione, in ottica sia proattiva e preventiva, sia nella gestione di un contesto emergenziale di prima accoglienza.

Positivi sono stati i feedback anche nei confronti dell'organizzazione, della location e dei servizi offerti per il corso.

Bibliografia

Ippolita, Tecnologie del dominio. Lessico minimo di autodifesa digitale, Milano, Meltemi, 2017.

Ippolita, Anime elettriche, Milano, Jaca Book, 2016

Ippolita, La rete è libera e democratica. Falso!, Laterza, 2014

Ippolita, Nell'acquario di Facebook, Milano, Ledizioni, 2012

Ippolita, Luci e ombre di Google. Futuro e passato dell'industria dei meta dati, Milano, Feltrinelli, 2007

Ippolita, Open non è free. Comunità digitali tra etica hacker e mercato globale, Milano, Eleuthera, 2005

Byung-Chul Han, La società della trasparenza, Roma, Nottetempo, 2014

Danah Boyd, It's complicated. La vita sociale degli adolescenti sul web, Roma, Castelvecchi, 2014

Carlo Formenti, Utopie letali, Milano, Jaka Book, 2013